DETAILED DESCRIPTION OF THE INVENTION

[0018] As noted in the background section, a rechargeable-power-supply (e.g., a rechargeable battery) that powers a device can be recharged by a recharging mechanism (e.g., recharge-circuit). Devices that are powered by a rechargeable-power-supply provide a mechanism for recharging the rechargeable-power-supply. These devices (e.g., portable electronic devices, mechanical toys) are generally valuable and/or may contain valuable data. Unfortunately, theft of more popular electronic devices such as the Apple iPod music-player has become a serious problem. In a few reported cases, owners of the Apple iPod themselves have been seriously injured or even murdered. Hence, techniques that can protect against unauthorized use and deter and reduce theft of such devices would be highly useful.

[0019] Accordingly, the invention pertains to techniques for protecting against extended unauthorized use of device. It will be appreciated that hindering the normal use and enjoyment of devices which are in use without proper authorization (e.g., disabling the ability of such devices to be recharged) can serve as a deterrent to theft. This should also result in a significant reduction of crime against the lawful owners of such devices.

[0020] In accordance with one aspect of the invention, when unauthorized use of a device is suspected, a recharging mechanism (e.g., recharge-circuit) of the device is disabled in order to guard against extended unauthorized use of the device. The recharging mechanism normally recharges the rechargeable-power-supply that powers the device. Consequently, normal use and enjoyment of the device can be significantly reduced when the recharger is disabled. Moreover, for devices that are mainly powered by a rechargeable-power-supply (e.g., music-players, phones, Personal Digital Assistants), disabling the recharger effectively renders the device inoperable when the power of the main power-supply has run out. Therefore, disabling the recharger should serve as a deterrent to theft.

[0021] In one embodiment, unauthorized use is suspected when an event, condition, or situation occurs (e.g., a timer expires, device is connected to a power-supply or another device, device is outside a determined geographical boundary). In any case, when unauthorized use is suspected, an authorization process can be initiated (e.g., an authorization-code or security-code may be requested). If the authorization process fails to authorize the user, the recharger mechanism is disabled so that it can no longer recharge the rechargeable-power-supply. The recharger may subsequently be enabled if the user can be authorized.

[0022] In accordance with another embodiment of the invention, a device can automatically detect whether it has been just connected to another component (e.g., adapter, personal computer) that has not been authorized. Hence, an authorization process may be initiated when the device is connected to an unauthorized device. However, a lawful owner of the device can configure and authorize devices that are known by a unique identifier (e.g., adapter-id, processor-id) and authorize a new device during the authorization process.

[0023] Another aspect of the invention pertains to techniques for detecting unauthorized use of devices. When a connection is made to a device, it is determined whether the device is authorized for use (e.g., has not been reported stolen, not out of a geographical boundary). Typically, devices make a connection to a service provider (e.g., server) to request services (e.g., down-load music, check account). As such, it is possible to check for unauthorized use of the devices based on various criteria. If unauthorized use of the device is suspected one or more operations can be performed to effectively hamper the normal use and enjoyment of the devices. These operations include: disabling the recharger mechanism, disabling the

[0024] Embodiments of these aspects of the invention are discussed below with reference to FIGS. **1A-5**. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

[0025] FIG. **1A** depicts a device **100** in accordance with one embodiment of the invention. The device **100** can, for example, be a personal computer, a portable device (e.g., personal computer, cell phone, Global Positioning System (GPS), media-player, wireless phone, personal digital assistant). As shown in FIG. **1A**, a rechargeable-power-supply **102** (e.g., a battery) and a recharger (e.g., a recharge-circuit) **104** are provided for the device **100**. Normally, the recharger **104** can be connected to a power source **106** in order to charge the rechargeable-power-supply **102**. In other words, the recharger **104** can charge the rechargeable-power-supply **102** when connected to the power source **106**.

[0026] It will be appreciated that a guardian **108** can disable the recharger **104** in order to effectively prevent the recharger **104** to charge the rechargeable-power-supply **102** even when the recharger **104** is connected to the power source **106**. Moreover, the guardian **108** can disable the recharger **104** when unauthorized use of the device is suspected. Unauthorized use can be suspected when, for example, an event, condition, or situation indicates that the device may be used without authorization. As will be described in more detail below, such an event, condition, or situation can, for example, be the expiration of a timer, connection of the device **100** to another object (e.g., another device, adaptor), or removal of the device from a geographical boundary. When such event, condition, or situation occurs, the guardian **108** may disable the recharger **104** so that the recharger **104** cannot charge the rechargeable-power-supply **102**. This significantly hampers the normal use and enjoyment of device **100**. If the rechargeable-power-supply **102** is the main source of power, disabling the recharger **104** would render the device effectively useless as it cannot be operated without power supply. It will be appreciated that among other things, this would serve as a theft deterrent.

[0027] It should be noted that if the guardian **108** determines that the use of the device **100** is authorized, it does not disable the recharger **104**. By way of example, when a timer has expired, the guardian **108** can prompt for a security-code (e.g., password) which if entered correctly, would result in setting the timer again (e.g., for 30 days) without disabling the recharger **104**. Alternatively, the guardian **108** can, for example, be configured to automatically disable the recharger **104** when an event, condition, or situation occurs (e.g., a timer expires). In such cases, the guardian **108** would